Indice

1 Introduzione

L'attuale tecnologia permette di sviluppare calcolatori elettronici sempre più potenti. Questo incremento però non potrà essere infinito, in quanto i calcolatori attuali sono limitati dall'essere costruiti secondo leggi fisiche ben definite, che sono quelle della fisica classica. Secondo la Legge di Moore degli anni sessanta, la potenza computazionale sarebbe raddoppiata una volta ogni due anni. Recentemente però lo stesso personaggio ha specificato che questo fenomeno si fermerà nei prossimi dieci anni.
L'introduzione di un nuovo paradigma scientifico, ossia la *meccanica quantistica* permetterà, secondo molti scienziati, di sfuggire alla limitatezza degli attuali calcolatori.
Un computer quantistico non è un'evoluzione di quello classico ma è una macchina del tutto differente sia nell'aspetto che nei contenuti. Attualmente non sono disponibili esempi di calcolatori quantistici completi, ma sono stati svolti soltanto esperimenti in laboratorio relativi a semplici e limitati algoritmi.
L'introduzione della computazione quantistica stravolgerà completamente l'informatica, e il trattamento dell'informazione, in quanto permetterà di risolvere problemi scientifici che sono attualmente irrisolvibili.
Un aspetto preoccupante riguarderà la crittografia classica che è basata sulla attuale limitatezza computazionale. Essa non riuscirà più a fornire un adeguata sicurezza ad attacchi crittoanalitici quantistici. L'introduzione di questi nuovi calcolatori non rappresenterà soltanto quindi un semplice aumento di velocità, ma un grosso stravolgimento dell'attuale modo di scrivere e concepire algoritmi.
Questa breve relazione mira a mettere in luce questi argomenti, fornendo una piccola introduzione a questo nuovo campo della ricerca scientifica.

2 Breve storia dei calcolatori quantistici

La computazione classica si basa sul modello astratto della Macchina di Turing, definito nel 1936 dal matematico inglese A. Turing e successivamente rielaborato da John von Neumann negli anni '40.
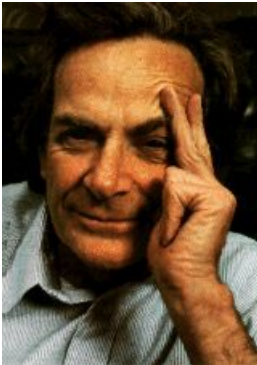
Figura 1: R. Feynman

Successivamente R. Feynman dimostrò che nessuna Macchina di Turing classica poteva simulare certi fenomeni fisici senza incorrere in un rallentamento esponenziale delle sue prestazioni. Al contrario, un "simulatore quantistico universale" avrebbe potuto effettuare la simulazione in maniera più efficiente.

Figura 2: D. Deutsch

Nel 1985 D. Deutsch formalizzò queste idee nella sua Macchina di Turing Quantistica Universale, che rappresenta in teoria della calcolabilità quantistica esattamente quello che la Macchina di Turing Universale rappresenta per la calcolabilità classica e ha portato alla concezione moderna di *computazione quantistica*.

Figura 3: P. Shor

L'introduzione del nuovo modello di calcolo ha provocato degli effetti nel campo della complessità computazionale, (come previsto da Feynman). Infatti, nel 1994 P. Shor dimostra che il problema della fattorizzazione dei numeri primi (classicamente considerato intrattabile) si può risolvere efficientemente (cioè in tempo polinomiale) con un algoritmo quantistico.

3 Fisica quantistica: nozioni di base

Le idee che costituiscono la *fisica quantistica* o *meccanica quantistica* risultano essere differenti rispetto a quelle classiche. I postulati che concretizzano queste idee rappresentano un nuovo modo di guardare la realtà interpretando i fenomeni che

accadono a livello microscopico.
Quello che portò allo studio di una meccanica differente da quella classica fu lo studio dello spettro del corpo nero e dell'effetto fotoelettrico. La scoperta realmente interessante è stata quella sullo spettro del corpo nero perché ha permesso di quantizzare l'energia.
Mentre lo studio dell'effetto fotoelettrico suggeriva che la radiazione elettromagnetica avesse un duplice comportamento (ondulatorio e corpuscolare) durante i processi di interazione con la materia

3.1 Concetto di quanto di Planck

L'introduzione del concetto di quanto avvenne nell'ambito degli studi sulla radiazione dei corpi neri, ovvero corpi ideali capaci di assorbire completamente la radiazione incidente. I grafici sperimentali ottenuti dall'analisi dell'emissione di radiazione elettromagnetica di un corpo incandescente erano infatti in contrasto con le previsioni teoriche della fisica classica.
Planck cercò un modello fisico che potesse giustificare questo fenomeno. Egli ipotizzò che l'interazione tra radiazione e materia avvenisse per trasferimento di quantità finite di energia che chiamò *quanti*, ciascuno dotato di energia pari a hf, dove f rappresenta la frequenza e h è ora noto come costante di Planck.

3.2 Contributo di Einstein

Successivamente Albert Einstein ricorse al concetto di *quanto* introdotto da Planck per spiegare l'effetto fotoelettrico, il fenomeno per cui una superficie metallica colpita da radiazione elettromagnetica di opportuna frequenza emette elettroni.
Secondo la teoria classica l'energia degli elettroni emessi doveva dipendere dall'intensità della radiazione; ma le osservazioni sperimentali mostrarono che l'intensità della radiazione incidente influiva sul numero di elettroni emessi ma non sulla loro energia; questa risultò invece dipendere dalla frequenza della radiazione: all'aumentare della frequenza aumentava l'energia degli elettroni emessi. Inoltre, in corrispondenza di frequenze inferiori a un valore critico, non si osservava alcuna emissione di elettroni.
Einstein spiegò questi risultati descrivendo il fenomeno come un insieme di urti tra i fotoni(quanti della radiazione elettromagnetica) e gli elettroni del metallo: durante l'urto un

fotone cede la su energia ad un elettrone del metallo provocandone l'estrazione; essendo poi l'energia del fotone proporzionale alla frequenza della radiazione, ciò avviene anche per l'energia dell'elettrone emesso.
Poiché i fotoni sono discontinui non è possibile utilizzare una teoria classica deterministica ma una di tipo probabilistico e statistico. Quindi si deve rinunciare a definire le leggi in maniera deterministica e si può cogliere solo delle ricorrenze statistiche e fare ipotesi basate sul calcolo dello probabilità.
Quindi la meccanica quantistica fornisce informazioni sulle probabilità di misurare un dato valore, il che può essere interpretato come: avendo a disposizione infiniti sistemi identici, effettuando la stessa misura su tutti i sistemi, la distribuzione dei valori ottenuti è proprio il modulo quadro della funzione d'onda che descrive il sistema. Quest'ultima fornisce quindi la densità di probabilità per la localizzazione di una particella.

4 Il quantum bit

In un computer quantistico l'unità fondamentale di informazione è il *quantum bit* o *qubit.* Per spiegare questo nuovo concetto dobbiamo fare uso di una notazione matematica, conosciuta come *notazione di Dirac*. Per rappresentare lo stato di un qubit si utilizza un vettore unitario in uno spazio vettoriale complesso a due dimensioni. Lo stato di un bit classico viene descritto mediante i valori *0* ed *1,* analogamente per il qubit si utilizzano i vettori $|0\rangle$ e $|1\rangle$. Usando la notazione classica dell'algebra lineare possiamo rappresentare $|0\rangle$ con il vettore $(1,0)^T$ e $|1\rangle$ con il vettore $(0,1)^T$, nella notazione classica invece si indicano formalmente nel seguente modo:

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

insieme formano la base ortonormale per C^2

$$\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}$$

Dove il vettore colonna si indica con $|\rangle$ e viene chiamato "*bra",* mentre il vettore riga si indica con $\langle|$ e si indica con *"ket"*, insieme formano il *braket*.
La differenza tra bits e qubits sta nel fatto che un qubit si può trovare anche in altri stati

diversi da $|0\rangle$ e $|1\rangle$.

Il braket rappresenta la combinazione lineare

$$|\psi = \alpha|0\rangle + \beta|1\rangle$$

dove *α* e *β* sono numeri complessi tali che

$$|\alpha|^2 + |\beta|^2 = 1$$

rappresentante un possibile stato del qubit.

Mentre ad un bit classico corrispondono due stati fisici precisi quali *0* e *1*, nel qubit non è possibile misurare con precisione il suo stato quantistico, cioè i valori *α* e *β*. Possiamo solo associare una probabilità pari a $|\alpha|^2$ di essere in $|0\rangle$ oppure pari a $|\beta|^2$ di essere in $|1\rangle$, questi due valori sono quindi ampiezze di probabilità.

Ad esempio un qubit si può trovare nello stato

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

nel momento in cui lo misuriamo il risultato sarà nel 50% dei casi a *1* e per il restante 50% a *0*.

4.1 Interpretazione fisica di un quantum bit

Alla descrizione matematica di qubit corrisponde nella realtà un qualsiasi sistema fisico con almeno due livelli di energia distinti e adeguatamente separati. Comunemente esistono tre approcci:

- L'allineamento di uno spin nucleare in un campo magnetico uniforme;
- Due diverse polarizzazioni di un fotone;
- Due livelli di energia discreti di un elettrone orbitante in un singolo atomo;

Un esempio classico è dato dall'atomo di idrogeno H^2 dove si fa corrispondere al primo livello di energia *(n = 0)* lo stato $|0\rangle$, mentre al livello di energia *(n = 1)*, cioè lo stato eccitato dell'elettrone, lo stato $|1\rangle$.
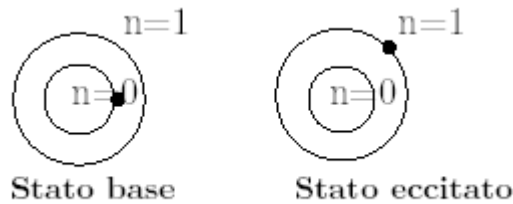
Figura 4:Qubit rappresentato da un elettrone in un atomo d'idrogeno

Quando misuriamo lo stato del qubit lo facciamo collassare dalla sua sovrapposizione di | $|0\rangle$ e $|1\rangle$ allo stato specifico consistente, in quanto con la misura varia lo stato del sistema.

5 La potenza dei calcolatori quantistici

La potenza dei calcolatori quantistici è decisamente superiore a quella dei normali calcolatori, e mostreremo questo tramite un esempio.

Si consideri un registro composto da 3 bit. Con questo possiamo rappresentare fino a 8 diversi numeri possibili, cioè le rappresentazioni binari dei numeri da 0 a 7. Consideriamo ora un registro quantistico composto da 3 qubit. Esso sarà in grado di contenere fino a tutti gli 8 numeri contemporaneamente grazie ad una sovrapposizione quantistica, cioè tramite una *sovrapposizione* coerente di stati; infatti in questo stato, conosciuto come *superposition* o *blend*., il qubit esiste sia come 0 che 1. E' questa proprietà del qubit che ci permette di avere un'alta potenza di calcolo. L'unico problema è che in realtà possiamo misurare soltanto uno stato alla volta, consentendoci comunque di manipolare più qubit alla volta e poi osservare il risultato. Altro problema che si pone è la *decorrenza*, cioè il riuscire a manipolare questi qubit senza interferire con il loro stato. Normalmente si vorrebbe ottenere i qubit isolandoli e permettendo le interazioni soltanto tra di essi, ma non è di facile realizzazione. Per risolvere questo problema ci si può rifare alla teoria dell'informazione di Shannon ed inserire dei sistemi di correzione dell'errore.

In un calcolatore tradizionale l'informazione viene ricavata attraverso il passaggio dei bit dalle cosiddette porte logiche, analogamente si può parlare di *quantum gates* che

manipolano normalmente uno o più qubit.
L'informatica ci insegna che è possibile, a puro livello teorico, simulare un calcolatore quantistico tramite un normale calcolatore. In pratica però non è realizzabile perché il livello di correlazione tra quantum bits è qualitativamente diverso da quello dei bits.
Molti studiosi hanno cercato quindi di sviluppare algoritmi per risolvere compiti complessi su calcolatori quantici. Ad esempio Peter Shor, ricercatore alla AT&T Bell Laboratories in New Jersey, è stato il primo a sviluppare un algoritmo per questa tipologia di macchina. Lui ed altri ricercatori, come quelli dell'IBM, intendono sfruttare il quantum computing per fattorizzare grossi numeri.
La potenza di computazione dei calcolatori quantistici è di alto interesse perché permetterebbe di risolvere complessi calcoli scientifici e potrebbe anche indebolire tutti gli algoritmi sviluppati con i principi dell'attuale crittografia, spesso basati appunto sul problema matematico della fattorizzazione. La crittografia moderna si basa sul fatto che il procedimento per nascondere i dati è computabile mentre quello per rivelarli non è, con dei calcolatori classici, computazionalmente possibile senza l'opportuna chiave segreta. L'arrivo dei computer quantistici pone il problema di migliorare e trovare soluzioni alternative alla classica crittografia asimmetrica. Una di queste proposte che fa uso della meccanica quantistica verrà discussa in seguito.

6 **Complessità computazionale**

Nella computazione classica abbiamo principalmente due classi di complessità temporale: la classe P e quella NP. Nella prima si hanno tutti i problemi che si possono risolvere efficientemente, cioè mediante un algoritmo deterministico in tempo polinomiale nella dimensione dei dati, mentre la seconda comprende tutti quei problemi risolvibili da una macchina di Turing non-deterministica in tempo polinomiale.
Un'altra importante classe di complessità è denotata con il nome PSPACE, dove però si fa riferimento allo spazio.
I risultati finora ottenuti in complessità computazionale stabiliscono la seguente relazione gerarchica:

$$P \leqslant NP \leqslant PSPACE$$

Con l'introduzione degli algoritmi stocastici è stata introdotta una nuova classe chiamata BPP (Bounded Polynomial Probabilistic). Questa classe comprende tutti quei problemi che si possono risolvere in tempo polinomiale e con una probabilità di errore piccola.
La teoria della complessità computazionale quantistica fa riferimento al Modello della Macchina di Turing Quantistica. In questo contesto si è definita la classe BQP che comprende tutti i problemi che si possono risolvere con una probabilità di errore piccola usando un circuito quantistico polinomiale. Il risultato ottenuto fino ad ora è il seguente:

$$BPP \leqslant BQP \leqslant PSPACE$$

La Macchina di Turing Quantistica

Per spiegare il comportamento di una Macchina di Turing Quantistica (QTM) introduciamo il concetto di Macchina di Turing Probabilistica (PTM).
La computazione di una PTM *M* può essere descritta attraverso un grafo dove:

- i nodi sono le configurazioni di M
- esiste un arco di peso p $\in$ [0, 1] dal nodo c_i al nodo c_j se la transizione $c_i \rightarrow c_j$ accade con probabilità p.
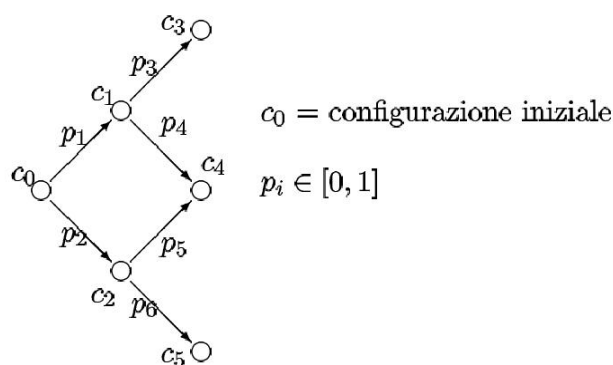
Figura 5: Stati di una PTM

Attraverso una funzione di transizione β della macchia *M* si deduce la probabilità associata agli archi.

β t.c. (somma dei pesi di tutti gli archi uscenti da un nodo) = 1

Dopo due passi di computazione, *M* si troverà nella configurazione

c_3 con probabilità p_1 p_3 = s_3

c_4 con probabilità $p_1 p_4 + p_2 p_5 = s_4$

c_5 con probabilità $p_2 p_6 = s_5$

quindi si trova in una *sovrapposizione di configurazioni*.

$$|\Psi\rangle = s_3|c_3\rangle + s_4|c_4\rangle + s_5|c_5\rangle$$

Quindi la macchina M al tempo t si troverà nello stato

$$|\psi(t)\rangle = \sum_{i \in N} s_i |c_i\rangle$$

Possiamo costruire una matrice *U* in cui l'elemento in posizione *(i, j)* rappresenta la probabilità di passare dalla configurazione c_j alla configurazione c_i.

Allora *t* passi di computazione di *M* si esprimono con

$$|\psi(t)\rangle = U^t |\psi(0)\rangle$$

dove $|\psi(0)\rangle = |0\rangle$ è la sovrapposizione iniziale di *M*.

Analogamente una QTM *Q* è definita in maniera del tutto analoga ad una PTM *M*, con la differenza che la probabilità di passare da una configurazione all'altra è data dal quadrato del modulo di un numero complesso chiamato ampiezza della transizione.
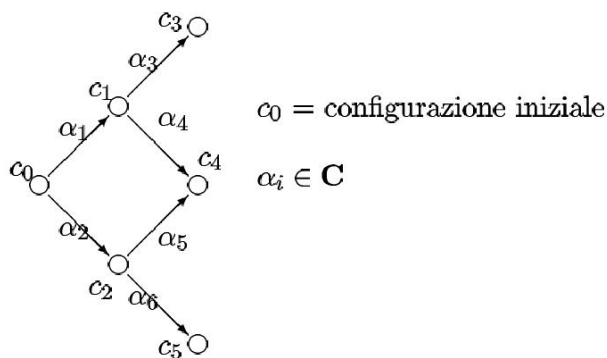
Figura 6: Stati di una QTM

Ad esempio :

l'ampiezza della transizione $c_1 \rightarrow c_2$ è $\alpha_1 \in C$

la corrispondente probabilità è $|\alpha_1|^2$

$$\sum_{i=1}^{k} |\alpha_i|^2 = 1$$

Analogamente, dopo due passi di computazione la macchina Q si troverà in

c_3 con ampiezza $\alpha_1 \alpha_3 = \gamma_3$ e probabilità $|\gamma_3|^2$

c_4 con ampiezza $\alpha_1 \alpha_4 + \alpha_2 \alpha_5 = \gamma_4$ e probabilità $|\gamma_4|^2$

c_3 con ampiezza $\alpha_2 \alpha_6 = \gamma_5$ e probabilità $|\gamma_5|^2$

Ad ogni istante t, la macchina Q si trova nella sovrapposizione

$$|\Psi(t)\rangle = U^t |\Psi(0)\rangle$$

dove l'elemento *(i, j)*esimo di *U* è ora l'ampiezza della transizione $c_j \rightarrow c_i$.

Poniamo ora che Q al tempo *t* si trovi nella sovrapposizione $|\Psi(t)\rangle = \gamma_1 |c_1\rangle + \gamma_2 |c_2\rangle$

.
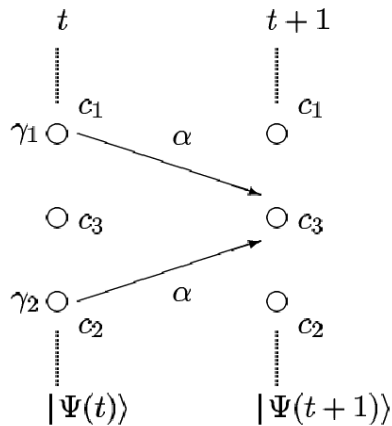
Figura 7: Transizione da una configurazione c_i ad una c_j

All'istante t troveremo Q in c_1 (c_2) con probabilità $|\gamma_1|^2$ ($|\gamma_2|^2$). La probabilità p_1 che all'istante successivo Q assuma la configurazione c_3 si ottiene che

$$p_1 = |\alpha|^2 (|\gamma_1|^2 + |\gamma_2|^2)$$

Al tempo t + 1 la probabilità p_2 di osservare la macchina nella configurazione c_3 sarà da cui

$$p_2 = |\alpha|^2 |\gamma_1 + \gamma_2|^2$$

essendo $\alpha(\gamma_1 + \gamma_2)$ l'ampiezza di c_3. Chiaramente $p_1 \neq p_2$.

7 Algoritmi quantistici

7.1 Algoritmo di Grover

Nel 1996 Lov Grover introdusse un metodo quantistico per risolvere problemi di ricerca non strutturati fornendo un miglioramento quadratico rispetto alle prestazioni degli algoritmi di ricerca classici esistenti.
Un problema di ricerca strutturato è un problema di ricerca dove si conosce la struttura dello spazio delle soluzioni e si sfrutta quest'informazione per costruire algoritmi efficienti. Invece un problema di ricerca non strutturato è caratterizzato dal fatto che non si conosce la struttura dello spazio delle soluzioni.
Nel caso generale di un problema di ricerca non strutturato, il miglior algoritmo classico che si possa applicare è quello di scandire tutti gli elementi dello spazio di ricerca finché non si è trovata la soluzione. Questo modo di procedere ha una complessità di $O(N)$ dove N è il numero degli elementi dello spazio di ricerca. Tuttavia, su un computer quantistico, questo tipo di problema si può risolvere con una complessità pari a $O(\sqrt{N})$ utilizzando il metodo di Grover.

7.2 Algoritmo di Shor

Un problema molto conosciuto è quello della fattorizzazione degli interi, cioè dato un numero composto N trovare i suoi fattori primi in tempo polinomiale. Determinare se un numero è primo o composto è invece un problema computazionalmente facile; infatti l'algoritmo probabilistico di Miller-Rabin, per il test di primalità, impiega $O(s \log N)$ operazioni con un errore pari a $E \leq 2^{-s}$. Nell'estate del 2002 tre ricercatori indiani hanno scoperto anche un algoritmo deterministico per il test di primalità che opera in tempo polinomiale.

Determinato se un numero è primo o no, ricavarne i suoi fattori non è altrettanto facile, e tutti i sistemi crittografici più diffusi, come ad esempio RSA, sfruttano la credenza di molto scienziati che non esista un algoritmo polinomiale per la fattorizzazione, o che se esista sia computazionalmente difficile. Il più efficiente algoritmo (non quantistico) per la fattorizzazione si chiama *number field sieve* e possiede una complessità superpolinomiale. Peter Shor ideò a metà degli anni 90 un algoritmo quantistico capace di fattorizzare un numero intero composto in tempo polinomiale nel numero di cifre $O(\log N)$ in N. L'algoritmo si compone di cinque passi ed in cui solo il terzo passo dev'essere computato tramite l'ausilio di un computer quantistico.
Per la comprensione di questo algoritmo introdurremo un riassunto dei concetti di teoria dei numeri a noi necessari per spiegarne il funzionamento.

7.2.1 Ordine di un numero

Dati due numeri interi positivi a ed N coprimi tra loro e tali che $a < N$, si definisce l'*ordine di a modulo N* come il più piccolo intero r tale che $a^r = 1 (\mathrm{mod}\ n)$. In letteratura non sono presenti algoritmi classici che permettano di determinare r in tempo polinomiale. Descriveremo in seguito un algoritmo quantistico che permette di risolvere questo problema con una complessità $O(L^3)$.

7.2.2 Aritmetica modulo *n*

Dato un intero positivo n ed un intero a, se si divide a per n, si ottiene un quoziente intero q ed un resto (o residuo) intero r ubbidienti alla seguente relazione:

$$a = qn + r$$

$$\text{con} \quad 0 \le r < n \quad \text{ed} \quad q \ge 0$$

Le operazioni dell'aritmetica modulo n sono le operazioni aritmetiche di somma, sottrazione, moltiplicazione e divisione dove si prende il risultato modulo n. E' importante notare che mentre nell'aritmetica classica gli unici interi che possono avere un inverso sono -1 ed 1, nell'aritmetica modulare esistono altri interi che possiedono un inverso.

Un intero a in modulo n ha un inverso modulo n se e solo se $MCD(a, n) = 1$, dove $MCD(a,n)$ è il massimo comun divisore di x ed n.

7.2.3 Algoritmo di Euclide

Per calcolare dati *a* e *b* il massimo comun divisore *MCD(a,b)*, utilizziamo l'Algoritmo di Euclide. Tale algoritmo si basa sul teorema che afferma che per ogni intero non negativo *a* ed ogni intero positivo *b* vale:

$$mcd(a,b) = mcd(b, a \bmod b)$$

questo si dimostra che supposto $d = mcd(a,b)$ allora per definizione di massimo comune divisore si avrà che *d* divide *a* e che *d* divide *b*. Questo si può esprimere formalmente con:

$$a = kb + r \equiv r \bmod b$$

$$a \bmod b = r$$

con *k* e *r* interi. Quindi vale $(a \bmod b) = a - kb$ per qualche intero *k*. Ma dato che *d* divide *b*, divide anche *kb*. Si ha anche *d* divide *a*, quindi *d* divide *(a mod b)*. Sì dimostra in tal maniera che *d* è un divisore comune di *b* e *(a mod b).* Similmente se *d* è divisore comune di *b* e *(a mod b)*, allora *d* divide *kb*, questo significa che *d* divide [*kb + (a mod b)],* che è equivalente a *d* che divide *a*. Per tanto l'insieme dei divisori comuni di *a* e *b* è uguale all'insieme dei divisori comuni di *b* e *(a mod b)*, si giunge quindi a dire che il massimo comune divisore di una coppia è equivalente al massimo comuni divisore dell'altra coppia, dimostrando il teorema.

L'algoritmo di Euclide presenta la seguente procedura:

EUCLIDE(a,b)

1. A := a; B := b
2. **If** B == 0 **return** A = mcd(a,b)
3. R := A mod B
4. A := B
5. B := R
6. **goto** 2

La complessità dell'algoritmo è $O(L^3)$, dove *L* è il numero di bits necessari alla rappresentazione di *p* e *q*. Questo perché l'algoritmo richiede al più *O(L)* divisioni binarie, ciascuna delle quali richiede $O(L^2)$ operazioni sui bits.

7.2.4 Algoritmo di Shor

L'algoritmo in questione prevede dato un intero N di trovare un altro intero p compreso tra 1 ed N che divide N. Possiamo risolvere il problema in due parti:

1. Ridurre il problema della fattorizzazione ad un problema di ricerca dell'ordine, eseguita da un calcolatore classico.
2. Risolvere il problema di ricerca dell'ordine tramite un calcolatore quantistico.

Riduzione al problema di ricerca dell'ordine

Procediamo a descrivere la prima parte dell'algoritmo, quella che riduce il problema di fattorizzazione ad un problema di ricerca dell'ordine.

Questa riduzione si dimostra facilmente nella maniera seguente:

Sia N un numero composto e sia a in $\{1..N\}$ una soluzione non banale dell'equazione $x^2=1(mod\ N)$, cioè tale che $x \neq N - 1= -1(mod\ N)$.

Sia inoltre L il numero di bits necessari per rappresentare $N(L = \lceil logN \rceil).$

Allora almeno uno tra $MCD(x -1, N)$ e $MCD(x+1, N)$ è un fattore non banale di N che può essere calcolato in $O(L^3)$ passi.

Questo risultato normalmente si combina dimostrando un altro teorema che ci assicura di determinare con alta probabilità un fattore non banale di un qualsiasi numero N.

Per calcolare un fattore non banale di un intero N di L bits, dispari e composto, procediamo in tal maniera:

1. Si scelga un numero casuale x tra 1 e $N-1$.
2. Si calcoli mediante l'algoritmo di Euclide l'$MCD(x, N)$. Se $MCD(x,N) > 1$ allora si è trovato un fattore non banale di N. Altrimenti si procede con il passo 3.
3. Tramite l'algoritmo quantistico descritto dopo si trovi l'ordine r di x modulo N.
4. Se r è dispari, oppure r è pari e $x^{r/2} = -1(mod\ N),$ allora ritorniamo al passo 1.
5. Con l'algoritmo di Euclide si calcoli $MCD(x^{r/2} - 1, N)$ ed $MCD(x^{r/2} + 1, N)$ e se uno dei due interi calcolati risulta essere un fattore non banale di N, allora l'algoritmo termina con successo, altrimenti si ritorni ad 1.

Ricerca dell'ordine tramite l'algoritmo quantistico

Lo strumento di riferimento per la costruzione di algoritmi quantistici efficienti di riferimento è la *Trasformata di Fourier Quantistica(QFT).* Questa ha applicazioni anche in altri problemi che non hanno soluzione normalmente in NP.

I processi fisici possono essere normalmente espressi sia nel dominio dei tempi che nel dominio delle frequenze. La trasformata di Fourier è un metodo per passare dal dominio dei tempi a quello delle frequenze. Tramite la QFT possiamo trasformare una funzione di periodo r in una funzione che assume valori diversi da zero in corrispondenza solo dei multipli della frequenza $\frac{2\pi}{r}$. La *Trasformata di Fourier Discreta(DFT)* lavora su N punti scelti ad uguale distanza nell'intervallo $[0,2\pi)$ e restituisce una funzione il cui dominio sono i numeri tra 0 e N-1. La DFT di una funzione di periodo r è concentrata sui multipli di $\frac{N}{r}$, questo significa che se r divide N allora la funzione risultante avrà valori diversi da zero solo sui multipli di $\frac{N}{r}$ altrimenti la funzione assumerà valori non nulli anche su interi vicini ai multipli di $\frac{N}{r}$.

Nella notazione classica, la DFT prende in input un vettore di numeri complessi $x_0,x_1,...,x_{N-1}$ e restituisce il vettore trasformato $y_0, y_1,...,y_{N-1}$ definito da

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi jk/N}$$

La *Trasformata di Fourier Quantistica (QFT)* è una variante della versione della DFT dove N è una potenza di 2. La funzione QFT opera sulle ampiezze degli stati quantistici in modo simile alla DFT, se $|0\rangle,...,|N-1\rangle$ è una base ortonormale dello spazio degli stati.

La QFT è quindi definita come l'operatore lineare F che trasforma gli stati della base nel

seguente modo:

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle$$

Equivalentemente è possibile esprimere questo operatore come la matrice quadrata di grandezza *N* i cui elementi generici sono:

$$\frac{1}{\sqrt{N}} (e^{2\pi i/N})^{jk}$$

La Trasformata di Fourier è alla base di una procedura generica nota come *stima della fase* che permette di ricavare una stima degli autovalori di una matrice unitaria.

Procedura di ricerca dell'ordine quantistica

Questa procedura richiede l'uso di due registri quantistici. Il primo di input contiene *n* qubit nello stato iniziale $|0\rangle$, con *n* dipendente dall'accuratezza richiesta per la stima della fase, nonché dalla probabilità di successo richiesta. Il secondo registro di output viene inizializzato tramite un operatore unitario *U* così definito:

$$U|y\rangle = |xy(mod\ N)\rangle\ se\ 0 \leq y \leq N-1$$

$$U|y\rangle = |y\rangle\ se\ N \leq y \leq 2^L - 1$$

Si applica quindi al primo registro la seguente Trasformata di Fourier Quantistica:

$$|u_s\rangle \rightarrow \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{2\pi isk/r} |x^k (mod\ N)\rangle$$

dove *r* è l'ordine di *x* modulo *N* e *0 ≤ s ≤ r-1,* si dimostra quindi che $|u_s\rangle$ è un autovettore di *U* con autovalore $e^{2\pi is/r}$ infatti applicata alla sopraddetta sovrapposizione quantistica si ottiene $U|u_s\rangle = e^{2\pi is/r} |u_s\rangle$.

Effettuando una misurazione sul primo registro si rileva con una buona probabilità un approssimazione di un multiplo di *1/r,* e da questo si ottiene *r*. A questo punto si conclude la componente quantistica dell'algoritmo di Shor.

7.2.5.Conseguenze dell'algoritmo di Shor

L'algoritmo di Shor ha aperto nuove problematiche legate alla crittografia. Come precedentemente menzionato gli algoritmi per lo scambio di chiave, come RSA, basano la loro sicurezza sull'attuale difficoltà computazionale del problema della fattorizzazione. Con queste nuove scoperte tutto questo potrebbe decadere e rendere completamente inutili gli esistenti sistemi crittografici, resi vulnerabili da attacchi crittoanalitici di tipo quantistico. Possibili soluzioni proposte si stanno sviluppando con tecniche quantistiche, ad esempio il protocollo *BB84* per lo scambio di chiavi segrete sviluppato nei laboratori di ricerca IBM.

8 Ostacoli ai Calcolatori Quantistici

I calcolatori quantistici operano ad un livello infinitesimale della materia. A causa del loro dominio di applicazione sono facilmente soggetti a problemi di rumore ed interferenza. Sebbene a livello teorico siano stati studiati approfonditamente, invece a livello pratico ci sono ancora parecchi ostacoli verso la loro realizzazione. Nella manipolazione degli stati quantistici l'ambiente esterno va' ad inquinare i risultati, creando stati incoerenti e dando luogo al fenomeno conosciuto come *decoerenza (decoherence).* Questo fenomeno compromette le prestazioni della macchina e aumenta i problemi di costruzione legati ad essa.

Nei calcolatori classici i problemi legati al rumore elettromagnetico vengono sistematicamente curati tramite i codici di correzione degli errori, in questa maniera l'informazione viene sufficientemente ridondata in maniera tale che non vada persa nonostante il segnale venga sostanzialmente degradato (ad esempio tramite i codici di Hamming).

La correzione d'errore non è facilmente estendibile all'informazione codificata all'interno di un sistema quantico. Innanzitutto quest'informazione, a causa della natura degli stati, è difficilmente clonabile, rendendo arduo ridondare i dati al fine di preservarli. Un altro problema è il processo di rilevamento di un errore, in quanto dobbiamo effettuare una misura ed estrarre alcuni dati dal sistema quantico; ma questa misura potrebbe disturbare il sistema e modificare l'informazione in esso codificata.

Il numero massimo di operazioni eseguibili è dato tra il tempo di coerenza τ_Q (cioè l'intervallo durante il quale il sistema rimane quantisticamente coerente) e la durata della singola trasformazione unitaria $n_{op} = \tau_Q/\tau_{op}$, mentre la frequenza delle operazioni è $\lambda = 1/n_{op}$.

Sistema fisico	Tempo di coerenza	Durata dell'operazione unitaria	Numero di operazioni al secondo
Spin nucleare	$10^{-2} - 10^{8}$	$10^{-3} - 10^{-6}$	$10^{5} - 10^{14}$
Spin dell'elettrone	10^{-3}	10^{-7}	10^{4}
Trappola ioni (In+)	10^{-1}	10^{-14}	10^{13}
Elettrone in Au	10^{-8}	10^{-14}	10^{6}
Elettrone in GaAs	10^{-10}	10^{-13}	10^{3}
Quantum dot	10^{-6}	10^{-9}	10^{3}
Cavità ottica	10^{-5}	10^{-14}	10^{9}
Cavità a microonde	10^{0}	10^{-4}	10^{4}

Tabella 1: Sistemi fisici, tempi di coerenza e operazioni al secondo

Mostriamo una tabella che fornisce alcuni valori del numero di operazioni al secondo a seconda delle varie proposte di sistema fisico per la realizzazione di un calcolatore quantistico:

Questi numeri indicativi mostrano come a seconda del sistema utilizzato ci siano grosse differenze nel numero di operazioni possibili. L'implementazione pratica esige che il tempo di esecuzione sia inferiore al tempo di coerenza, altrimenti diventa impossibile portare a termine il compito. Altro problema è realizzare procedure che siano più efficienti di quelle classiche.

L'idea della ridondanza può essere applicata però anche ai qubit, sfruttando più qubit correlati tra loro, e monitorando eventuali cambiamenti e comportamenti anomali. Gli esperimenti condotti hanno mostrato che sebbene nei calcolatori quantistici ci sia una grossa diffusione di errori ed imprecisione, almeno è possibile rilevarli e correggerli.

9 Linguaggio di programmazione quantistica

Con il passare del tempo sono state create le basi per lo sviluppo di proposte di linguaggio

di programmazione d'alto livello per i computer quantistici, come ad esempio:

- Q-gol (Greg Baker, 1996)
- qGCL (Paolo Zuliani, 2000)
- Quantum C Language (Stephen Blaha, 2002)

Il più evoluto progetto si è dimostrato quello di Zuliani il quale ha proposto un formalismo astratto con rigide regole semantiche.

L'obiettivo è quello di sviluppare un linguaggio che permetta di operare con i computer quantistici facendo uso di un formalismo simile a quello dei linguaggi esistenti (ad esempio con una una sintassi simile al C).

Nella seguente tabella vengono mostrate le principali differenze tra un linguaggio di programmazione classico ed un linguaggio quantistico

Linguaggio classico	Linguaggio quantico
Architettura classica	Architettura quantistica
Variabili	Registri quantistici
Input classico	Misurazione quantica
Espressioni booleane	Condizioni quantiche

Tabella 2: Differenze tra un linguaggio classico ed uno quantistico

9.1 Un esempio di programmazione

Un esempio di applicativo per un linguaggio di programmazione quantistica è `qlc`. Utilizza una sintassi molto simile a quella del C. Per capire meglio mostriamo alcuni comandi.

```
$ qcl --bits=5
[0/8] 1 |00000>
qcl> qureg a[1];
qcl> dump a
: SPECTRUM a: |....0>
1 |0>
```

In questo modo abbiamo eseguito i seguenti passi:

- utilizziamo con 5 qubits;
- lo stato della macchina è inizializzato a zero (|00000>);
- `qureg a[1]` alloca un bit per a.
- Il comando `dump  a` ci da informazioni su a, in particolare ci dice:

- SPECTRUM ci dice dove i qubits per a sono stati allocati.
- Dovremmo misurare il valore 0 con probabilità 1.

Ad esempio applichiamo l'operatore Not ed otteniamo la seguente situazione:

```
qcl> Not(a);
[2/8] 1 |00001>
```

Abbiamo trovato così il negato di a (da 0 a 1).

Testiamo ora l'operatore CNot(x,y). Il comportamento dell'operatore è così descritto: viene valutato il valore di y e se è 1 allora viene modificato lo stato di x.

```
qcl> qureg b[2];
qcl> Not(b[1]);
[3/8] 1 |00100>
qcl> CNot(b[0], b[1]);
[3/8] 1 |00110>
qcl> dump b[0];
: SPECTRUM b[0]: |...0.>
1 |1>
qcl> dump b[1];
: SPECTRUM b[1]: |..0..>
1 |1>
```

- Viene allocato lo spazio per b
- Si fa il Not
- Viene applicato l'operatore CNot
- Si verifica lo stato di b attraverso il comando dump.

E' importante lo sviluppo di linguaggi e di applicativi che permettano ai programmatori un facile cambiamento nel modo di pensare e di scrivere algoritmi. In modo tale da poter utilizzare al meglio le potenzialità che una macchina quantistica può offrire, anche senza avere grosse conoscenze fisiche.

10 Conclusioni

In questa relazione abbiamo cercato di dare un'idea di che cos'è un computer quantistico e di quello che può offrire. Questo nuovo campo di ricerca ha colto il nostro interesse in quanto punto di congiunzione tra diversi campi scientifici, principalmente Meccanica Quantistica e Teoria dell'Informazione.

Attualmente siamo lontani dalla realizzazione di computer quantistici completi, anche perché non tutti gli scienziati sono convinti di questa nuova tecnologia. Nonostante le perplessità di alcuni, nei laboratori dell'IBM, si è realizzato un primo calcolatore quantistico a 7 qubit capace di fattorizzare il numero 15.

Abbiamo voluto mettere in risalto anche la rivoluzione che questi nuovi calcolatori porteranno nei già esistenti sistemi informatici e crittografici, mostrando che sarà un cambiamento radicale nel fare algoritmi e sicurezza.

Riferimenti

1. Alessandra Di Pierro, *Quantum Computing: Appunti delle Lezioni, (*2004).
2. P. W. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring, in Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press (1994).
3. Marco Ivaldi, *Introduzione al quantum computing,* Luglio (2002).
4. Bernhard Ömer, *Structured Quantum Programming,* (2003).
5. Stallings, *Cryptography and Network Security*, Prentice Hall. (2003).
6. Brad Huntting, *An Introduction to Quantum Computing,* University of Colorado (2001).
7. Benjamin Schumacher, *Quantum Computing, Lectures Notes, (1998).*
8. Andrew M. Steane*, Quantum Error Correction, Clarendon Laboratory, Oxford OX1 3PU, England. (1996).*